Will the Real Salt Typhoon Please Stand Up?

pylos.co/2025/07/23/will-the-real-salt-typhoon-please-stand-up/

Joe 07/23/2025

On 17 July 2025, Bloomberg (no stranger to interesting information security reporting) issued a gated report on a non–public Recorded Future item related to Salt Typhoon activity. As previously noted in this space, Salt Typhoon operations are both incredibly significant given their targeting and scope, while also poorly understood and documented given the paucity of detailed public information on their operations. The Recorded Future report (or at least subsequent Bloomberg reporting on this report) would therefore appear to provide opportunities to improve our understanding of this threat actor.

Unfortunately, this is not the case. Admitting that the source report from Recorded Future is inaccessible therefore all following judgments are based on the Bloomberg exegesis, what actually emerges in public reporting is disconcerting with respect to People's Republic of China (PRC) cyber operations at large. The core argument stems from the second paragraph of the report:

> In the past five months, the Chinese state-sponsored hacking group widely referred to as Salt Typhoon has breached network devices at locations on the internet that are owned by the seven companies, including the American telecom and media firm Comcast Corp., South Africa's MTN Group Ltd. and South Korea's LG Uplus Corp., the report from cybersecurity firm Recorded Future Inc. shows. Bloomberg News reviewed the report under the condition that certain companies aren't named.

Yet the following paragraph in the Bloomberg article immediately shows there is far more going on here than compromise of telecommunication company (telco) backbone equipment:

> The report says the compromised devices likely belong to the seven companies' clients and doesn't say the telecommunications firms were breached.

The limitations of this are already obvious to readers, but despite the statement that the equipment in question is **not** telco-operated, backbone gear, the following conclusion is offered:

> Nonetheless, it shows the hackers' persistent efforts to infiltrate communications firms and their customers globally – and their success at penetrating the types of devices that have offered paths into organizations' networks in the past. In November, US officials

What is observed in this example is conflation between "victims in themselves" and "victims as a means to an end." Essentially, higher-end threat actors will compromise opportunistic, seemingly random endpoints wherever they can be found to build out proxy networks of hosts to channel and obfuscate subsequent operations. Compromising a telco end-user fits perfectly into this construct, and aligns with operations ranging from the KV Botnet to Flax Typhoon operations to Cyclops Blink.

This "means to an end" construct is demonstrated clearly in a following section, noting that service provider *clients*, and not the service provider itself, were compromised through this operation:

Salt Typhoon is a deeply concerning adversary that has demonstrated the willingness and ability to breach core network assets in major telco organizations for information and intelligence gathering. Yet this research appears to be linking Salt Typhoon to compromises of telco "end users" – the sort of small office and home office (SOHO) equipment frequently roped into botnets due to vulnerabilities and end-of-life circumstances. Previous, available reporting on Salt Typhoon has not noted the group targeting such equipment, at least not consistently nor at scale, leading to questions as to what is going on in the relevant analysis.

> Comcast said the hacked equipment belongs to a client, that it investigated and that its own network wasn't impacted. LG Uplus also said the breached device was owned by a client and the issue wasn't related to its internal systems. MTN said it hadn't detected any cyberattack by the group of hackers.

Notably, many *other* PRC entities very much engage in compromising SOHO devices. From the various botnet entities used by Volt Typhoon (such as the KV Botnet) to Flax Typhoon, PRC-linked threat actors (among other entities) have migrated much of their initial access and command and control infrastructure to proxy networks of compromised devices (sometimes referred to as "operational relay box" networks). These can include equipment

such as various internet of things (IoT) devices to SOHO networking appliances, but in nearly all cases devices that reside within the networks of larger telco organizations. Thus, if one were to research a Volt Typhoon firing node or a Flax Typhoon redirect box, autonomous system number (ASN) or network owner information would reflect that the entity involved was a Comcast, MTN, or similar organization.

The links to Salt Typhoon from this activity are thus—absent additional evidence—extremely flimsy given the much broader use of intermediate appliance or device compromise among many threat actors. Additionally, given Salt Typhoon's noted direction in compromising service provider backbone infrastructure to facilitate intelligence collection, it is extremely unclear how compromising Bob & Jane's Florist Netgear device would allow for any facilitation of subsequent targeting of the hosting ISP.

Quite simply: PRC-linked cyber actors are very definitely and aggressively targeting internet-connected equipment, SOHO, enterprise, or other, for exploitation. However, this specific exploitation almost certainly pertains to the creation of proxy networks for exploitation and subsequent command and control, and there remains no known instance of using such exploitation to "swim upstream" into the hosting telco's environment. The activity identified may certainly be associated with *eventual* Salt Typhoon operations, where such nodes are used to obfuscate network connections between operators and victims. But to think such activity reflects on the immediate risk to the hosting entities reveals a substantial lack of understanding of telco network segmentation and operations.

What has likely been identified in this case is not "Salt Typhoon targeting telcos" but rather Salt Typhoon (or other entities) building (or rebuilding) proxy networks to facilitate follow-on operations. This is NOT a trivial point in the slightest as identifying and, potentially, mitigating such proxy networks is a future, necessary step in getting ahead of emerging cyber intrusion activity. However, to draw a definitive line from "a potential Salt Typhoon operator compromised a SOHO router within Verizon ISP space indicates targeting of Verizon" is suboptimal, to say the least.

For the activity of specific interest then, what we are likely seeing is **a** PRC-linked entity (not necessarily Salt Typhoon) rebuild or reconstitute a proxy network of devices to be used or sold off for other operations. But to make a conclusion that such activity represents direct targeting of the hosting network is both unsupported by available evidence and ignores the actual architecture of ISP networks.

Nonetheless, the activity in question is concerning, but must be placed in the appropriate context for it to matter. Instead of harping on telco insecurity and vulnerability, the proper response to this activity is highlighting the very real risk entailed by the deployment and lack of maintenance of consumer equipment for internet connectivity. Such devices have been

marshalled into proxy networks to obfuscate adversary actions for many years, and acknowledging this vulnerability is critical to ensuring the security of many organizations at risk of state (or even criminal) exploitation.